

KODEX OCHRANY OSOBNÍCH ÚDAJŮ

Schválil (Approved by): podpis (signature): jméno (name): funkce (position):	Dipl.-Ing. Miroslav Hejna Člen představenstva	Označení: <i>Identification:</i>	LPT-IP-26
Ověřil (Verified by): podpis (signature): jméno (name): funkce (position):	Ing. Jan Hutira Finanční ředitel	Změna č.: <i>Revision:</i>	0
Zpracoval (Prepared by): podpis (signature): jméno (name): funkce (position):	Ing. Lucie Petráková Účetní	Datum vydání: <i>Issued on:</i>	25.5.2018
		Datum účinnosti: <i>Valid from:</i>	25.5.2018

Kodex ochrany osobních údajů – závazná směrnice

v souladu se zákonem č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů a Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES a směrnice Evropského parlamentu a Rady (EU) 2016/680 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů

Obsah

Kodex ochrany osobních údajů – závazná směrnice.....	2
1 Termíny	4
2 Předmět.....	5
3 Platnost a rozsah	5
4 Principy ochrany osobních údajů	6
5 Zvláštní případy zpracování údajů	9
6 Práva subjektů údajů	10
7 Proces řízení správy, zpracování a ochrany údajů/Odpovědnost za ochranu údajů	12
8 Komerový systém společnosti	14
9 Odpovědnost za porušení povinností stanovených tímto Kodexem	15
10 Změny kodexu	15

1 Termíny

Biometrické údaje

osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňují nebo potvrzují jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje.;

Citlivé údaje

osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, trestné činnosti, zdravotním stavu, sexuálním životě subjektu údajů, apod.;

Evidence osobních údajů

jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska.;

Genetické údaje

osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby.;

Likvidace osobních údajů

se rozumí fyzické zničení jejich nosiče, jejich fyzické vymazání nebo jejich trvalé vyloučení z dalšího zpracování.;

Nakládání s osobními údaji (zpracování)

je jakákoli operace či soubor operací prováděných s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů jako je jejich shromažďování, zaznamenávání, uspořádání, strukturování, organizace, ukládání, úpravy či změny, vyhledávání, konzultace, použití, zpřístupňování přenosem, šíření či poskytování jiným způsobem, seřazování či kombinování, blokování, mazání či likvidace. To zahrnuje i ruční zpracování osobních údajů ve strukturovaných složkách.;

Osobní údaje (údaje)

jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.;

Profilování

jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu.;

Příjemce

je jakákoli fyzická či právnická osoba, orgán veřejné správy, agentura či jakýkoli jiný subjekt, jemuž

jsou údaje zpřístupněny, ať již jde o třetí stranu či nikoli. Orgány veřejné správy, které mohou údaje případně obdržet v rámci jednotlivého dotazu, však nejsou za příjemce považovány.;

Správce údajů

je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení.;

Subjekt údajů

je jakákoli fyzická osoba, s jejímiž osobními údaji se nakládá.;

Třetí strana

je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jež je oprávněna ke zpracování osobních údajů.;

Zpracovatel údajů

je jakákoli fyzická či právnická osoba, orgán veřejné správy, agentura či jakýkoli jiný subjekt zpracovávající osobní údaje pro správce údajů (zpracování údajů prostřednictvím subdodavatele).;

Zvláštní kategorie údajů

jsou údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském či filozofickém přesvědčení, členství v odborech nebo o zdraví či sexuálním životě.

2 Předmět

Společnost za účelem přijetí těch nejvyšších a nejpřísnějších standardů na poli ochrany a nakládání s osobními údaji přijímá tento kodex a zavazuje se jej prosazovat ve svých interních záležitostech i vně společnosti, a to zejména ve styku se svými obchodními partnery a třetími osobami.

Tam kde je to možné, společnost tímto kodexem zavazuje své obchodní partnery i veškeré další osoby v souvislosti se správou a zpracováním osobních údajů.

Tento kodex upravuje a stanovuje práva a povinnosti společnosti jako celku při nakládání s osobními údaji a dalšími písemnostmi, které jsou předmětem ochrany osobních údajů, při jejich nakládání prostřednictvím interního informačního systému (dále jen „IS“), při jejich předávání / poskytnutí jiným subjektům apod. v souladu s relevantními právními předpisy.

3 Platnost a rozsah

1. Tento Kodex je směrnici, která je závazná pro celou společnost a nabývá účinnosti po jeho přijetí a publikaci managementem společnosti. Vztahuje se na nakládání s veškerými osobními údaji fyzických osob, zejména pak s údaji zákazníků, zaměstnanců, třetích stran, smluvních stran či obchodních partnerů.

2. Základní východiska:

- a) Níže uvedené principy mají za cíl zajistit vysoký stupeň ochrany údajů, a to jednotně pro celou společnost. Nenahrazují však požadované – a případně zákonné – podmínky, které musí být za účelem řádného nakládání s osobními údaji splněny. Tímto Kodexem nejsou dotčeny žádné povinnosti ani předpisy pro zpracování a použití osobních údajů vztahující se na společnost, jež jdou nad rámec níže uvedených principů či obsahují další omezení zpracování a použití osobních údajů.
- b) Shromážděné údaje musí být zpracovávány v souladu s právními předpisy, a to i v případě jejich předávání do zahraničí.
- c) Shromažďování osobních údajů a jejich předávání orgánům veřejné správy bude vždy prováděno – s výjimkou běžného smluvního vztahu se zákazníkem – v souladu se závaznými právními předpisy.
- d) Tento Kodex se řídí právem České republiky.

Kodex je závazný pro celou společnost a zvláště pak pro všechny zaměstnance společnosti, a to jak zaměstnance na základě pracovněprávního či jiného vztahu, kteří přicházejí nebo mohou přijít do styku s osobními či citlivými.

4 Principy ochrany osobních údajů

i. Transparentnost zpracování údajů

Informační povinnost

1. Subjektům údajů musí být umožněn snadný přístup k informacím týkajícím se náležitého nakládání s jejich osobními údaji, např. ze strany společnosti prostřednictvím publikace ochrany soukromí a osobních údajů a tohoto Kodexu.

Obsah a forma informací

1. Subjektům údajů musí být adekvátním způsobem poskytnuty následující informace:
 - a) informace o identitě správce (správců) údajů a kontakt na něj (ně);
 - b) informace o zamýšleném rozsahu a účelu shromažďování, zpracování a případně použití osobních údajů; tyto informace by měly zahrnovat bližší určení toho, jaké údaje se zaznamenávají, příp. zpracovávají/používají, proč, za jakým účelem a na jakou dobu;
 - c) informace o příjemci, rozsahu a účelu (účelech) předání v případě, že jsou osobní údaje předávány třetím stranám;
 - d) informace o způsobu zpracování, příp. použití údajů, zejména pak tehdy, mají-li být zpracovány či použity v zahraničí;
 - e) informace o zákonných právech subjektů údajů.
2. Bez ohledu na zvolené médium by měly být tyto informace subjektům údajů poskytnuty v jasné a snadno srozumitelné formě.

Dostupnost informací

1. Výše uvedené informace musí být subjektům údajů poskytnuty při jejich prvním shromáždění a následně při každém dalším vyžádání.

Souhlas

1. Není-li shromáždění, zpracování či použití údajů nutné pro účely zahájení či plnění smluvního vztahu či neexistuje-li k tomu žádné jiné oprávnění ze zákona, je nutné získat souhlas subjektu

údajů, a to nejpozději při zahájení shromažďování, zpracování či používání údajů.

2. Kromě výše uvedených informačních povinností je třeba dodržovat následující požadavky na souhlas subjektů údajů:

Souhlas a jeho forma

- a. Musí jít o souhlas výslovný, dobrovolný a informovaný tak, aby bylo subjektu údajů zejména zřejmé, v jakém rozsahu souhlas poskytuje a jaké jsou důsledky jeho neposkytnutí. Znění prohlášení o souhlasu musí být dostatečně přesné a musí subjekt údajů informovat o jeho právu vzít tento souhlas kdykoli zpět.
- b. Souhlas musí být získán v podobě adekvátní okolností (obvykle v podobě písemné či elektronické). Ve výjimečných případech může jít o souhlas ústní, pokud je dostatečně doloženo jeho poskytnutí a okolnosti, z nichž vyplývá, že ústní souhlas je postačující.

ii. Použití pro konkrétní účel

1. Osobní údaje nesmí být použity za jiným účelem než za účelem, k němuž byly původně poskytnuty.

Zákaz podmíněného souhlasu

1. Použití služeb či získání produktů, popř. služeb nesmí být podmíněno souhlasem subjektů údajů s použitím jejich údajů pro jiné účely, než je zahájení či plnění smluvního vztahu. To platí pouze tehdy, nemohou-li – či nemohou-li z rozumného hlediska – subjekty údajů využívat srovnatelné služby či srovnatelné produkty.

iii. Přesnost a minimalizace údajů

Přesnost – integrita a důvěrnost údajů

1. Osobní údaje musí být vždy správné a v potřebných případech musejí být průběžně aktualizovány (přesnost údajů).
2. S ohledem na účel (účely), za nímž jsou údaje shromažďovány, zpracovávány či využívány, by měla být přijata náležitá opatření, aby bylo zajištěno vymazání či případně oprava jakýchkoli nesprávných či neúplných informací.

Minimalizace - přiměřenost, zpracování údajů pouze v nutných případech, anonymizace a využití pseudonymů

1. Osobní údaje musí být s ohledem na jejich použití pro konkrétní účel přiměřené, relevantní a musí mít odpovídající rozsah (přiměřenost). V rámci konkrétního využití smí být údaje zpracovávány pouze tehdy, je-li to nutné (zpracování údajů pouze v nutných případech).
2. V případech, kdy je to možné a ekonomické, je třeba aplikovat procesy pro vymazání identifikačních znaků subjektů údajů (anonymizace) či jejich nahrazení jinými charakteristikami (využití pseudonymů). Při anonymizaci a využití pseudonymů je třeba postupovat tak, aby nebylo možné zjistit původní identitu subjektů údajů anebo aby to bylo možné pouze při vynaložení neúměrně velkého úsilí.

Profilace, statistické analýzy

1. Na základě příslušných nejmodernějších koncepcí či technologií je třeba aplikovat organizační a technická opatření s cílem zamezit zjištění profilů (např. profily pohybu, uživatelské profily, profily spotřeby). Výjimku tvoří případy, kdy to výslovně dovolují právní předpisy či kdy k tomu subjekt údajů poskytl předchozí souhlas.
2. Tento požadavek se nevztahuje na čistě statistické analýzy či studie na základě anonymizovaných údajů či údajů s využitím pseudonymů.

Archivace údajů

1. Při vytváření pravidel pro archivaci údajů je třeba zohlednit principy zpracování údajů, zejména pak princip přiměřenosti a princip zpracování údajů pouze v nutných případech. Osobní údaje nelze

archivovat bez výslovného souhlasu subjektu údajů, s výjimkou případů, kdy je to nutné z provozních důvodů či je to požadováno zákonem.

iv. Omezení dalšího předávání

Předávání údajů třetím stranám

1. Předávání osobních údajů třetím stranám je možné pouze na právním základě, například v případech, kdy je to nutné pro splnění smluvního požadavku vůči subjektu údajů či kdy k tomu subjekt údajů poskytl svůj souhlas.
2. Odstavec 1 se nevztahuje na případy, kdy existují národní omezení – zejména z důvodů bezpečnosti státu, národní obrany, veřejného pořádku či prevence, vyšetřování, odhalování a stíhání trestných činů – požadující předávání osobních údajů pro tyto účely.

Odpovědnost

1. Při předávání údajů třetím stranám, které nepatří mezi orgány veřejné správy, je společnost, resp. její pověřený zaměstnanec, povinna zajistit zpracování či využívání údajů v souladu se zákonem. Stejně tak je před předáním údajů potřeba s příjemcem projednat a odsouhlasit příslušná opatření pro zajištění ochrany a bezpečnosti údajů. V případě, kdy jsou uzavírány smlouvy se subjekty v zemích bez adekvátní úrovně ochrany údajů, je nutné zajistit dostatečné záruky s ohledem na ochranu práva na soukromí jednotlivce a výkon práv s tím spojených.
2. V souladu se všeobecně akceptovanými standardy je třeba přijmout příslušná technická a organizační opatření pro zajištění integrity a bezpečnosti údajů během jejich předávání třetí straně.

Zpracování údajů subdodavateli (zpracovateli)

1. Společnost spolupracuje s externími subdodavateli při plnění konkrétně specifikovaných činností, zejména se jedná o dodavatele zajišťující služby: ostrahu, dopravu, kontrolu pracovní neschopnosti zaměstnanců, zpracování mezd, vyúčtování cestovních náhrad, pracovní lékařské služby, služby v oblasti IT, BOZP a další. Tyto externí společnosti jsou povinni zachovávat mlčenlivost dle uzavřené smlouvy o zpracování osobních údajů.
2. V případě využití služeb subdodavatele musí smlouva kromě ujednání specifikující práci, kterou má subdodavatel vykonat, rovněž obsahovat povinnosti subdodavatele jakožto zpracovatele údajů. Tyto povinnosti budou obsahovat pokyny společnosti (správce údajů) v souvislosti s druhem a způsobem zpracování osobních údajů, účelem jejich zpracování a technickými a organizačními opatřeními potřebnými pro jejich ochranu.
3. Subdodavatel není bez předchozího souhlasu správce údajů oprávněn využít osobní údaje pro vlastní zpracovatelské účely či zpracovatelské účely třetích stran. V druhém uvedeném případě je třeba se s takovýmto subdodavatelem (subdodavateli) rovněž dohodnout na výše uvedených pravidlech.
4. Subdodavatelé jsou vybíráni podle schopnosti splnit výše uvedené požadavky.
5. Subdodavatelé plně spolupracují se společností na řádné správě, zpracování a ochraně osobních údajů v souladu se zákonem.
6. Subdodavatelé neprodleně hlásí společnosti jakékoli narušení ochrany osobních údajů. V případě neprodleného nenahlášení narušení ochrany osobních údajů ze strany subdodavatele tento odpovídá za veškeré sankce a škodu z toho vzniklou.

v. Ochrana údajů, organizace a bezpečnost údajů

Osoby odpovědné za ochranu údajů

1. Společnost v případě potřeby jmenuje osobu odpovědnou za ochranu osobních údajů (Data Protection Officer), jejímž úkolem je zajistit poučení jednotlivých oddělení o zákonných požadavcích a/nebo interních požadavcích společnosti a o strategii ochrany údajů a soukromí.

2. Osoba odpovědná za ochranu údajů se musí od počátečních fází účastnit vývoje nových produktů a služeb, aby bylo zajištěno, že budou v souladu s principy stanovenými v tomto Kodexu.

Kontrola úrovně ochrany údajů

1. V pravidelných intervalech by měla probíhat kontrola úrovně ochrany údajů (např. prostřednictvím auditu ochrany informací) za účelem přezkoumání efektivity a úspěšnosti implementovaných technických a organizačních opatření pro ochranu údajů. Takovéto audity může interně provádět osoba odpovědná za ochranu údajů či jiné organizační jednotky tímto úkolem pověřené. Jinou alternativou je provádění těchto auditů externí třetí stranou schválenou správcem údajů. Základem pro stanovení úrovně ochrany údajů jsou požadavky právních předpisů a firemní strategie ochrany údajů a požadavky tohoto Kodexu.

Technická a organizační opatření, opatření ve vztahu k zaměstnancům

1. Při zahájení práce ve společnosti musí být se zaměstnanci písemně sjednány závazky související se zachováním mlčenlivosti. Kromě toho musí být stanovena příslušná technická a organizační opatření pro nakládání s údaji v souvislosti s firemními procesy a IT systémy. V rámci takovýchto opatření je nutné:
 - a) zamezit přístup neoprávněných osob k systémům pro zpracování údajů, v rámci nichž jsou zpracovávány či využívány osobní údaje (regulace fyzického přístupu);
 - b) zajistit, aby neoprávněné osoby nemohly systémy pro zpracování údajů používat (regulace používání datových systémů);
 - c) zajistit, aby osoby oprávněné k používání systému pro zpracování údajů měly přístup výhradně k údajům, k nimž jsou oprávněny přistupovat, a aby neoprávněné osoby nemohly osobní údaje během zpracování či používání či po jejich zaznamenání číst, kopírovat měnit ani mazat (regulace přístupu k údajům);
 - d) zajistit, aby v průběhu elektronického přenosu či předávání či nahrávání údajů na datový nosič nemohly neoprávněné osoby osobní údaje číst, kopírovat, měnit ani mazat a aby bylo možné prozkoumat a stanovit, v jakých případech mají být údaje přenášeny prostředky pro přenos dat (regulace přenosu dat);
 - e) zajistit, aby bylo možné zpětně přezkoumat a zjistit, zda a kým byly osobní údaje do systémů pro zpracování údajů zadány, v těchto systémech změněny či z nich odstraněny (kontrola zadávání údajů);
 - f) zajistit, aby osobní údaje zpracovávané subdodavatelům byly zpracovávány pouze v souladu s pokyny objednatele (kontrola subdodavatele);
 - g) zajistit ochranu osobních údajů proti náhodnému zničení či ztrátě (zajištění dostupnosti údajů);
 - h) zajistit, aby údaje shromážděné pro různé účely byly zpracovávány odděleně (pravidlo odděleného zpracování údajů).

5 Zvláštní případy zpracování údajů

Přímý marketing

1. Subjekty údajů musí být informovány, že mohou kdykoli odmítnout použití svých osobních údajů pro účely přímého marketingu. Dále musí být informovány o povaze a obsahu takové komunikace a období, po které mohou být jejich údaje pro účely přímého marketingu využívány.
2. Subjekty údajů musí být informovány o právu odmítnout využívání svých osobních údajů pro účely přímého marketingu vždy, když takováto sdělení či materiály obdrží. Dále musí být subjektům údajů poskytnuty přiměřené nástroje pro uplatnění práva, aby jim nebyla takováto sdělení či materiály zasílány a musí být informovány zejména o tom, komu mohou takovéto odmítnutí adresovat.
3. Zvláštní právní ustanovení tohoto Kodexu, podmiňující použití osobních údajů souhlasem příslušných subjektů údajů, mají přednost před jinými ustanoveními.

Automatizovaná individuální rozhodnutí

1. Rozhodnutí, která hodnotí jednotlivé aspekty určité osoby a mohou s sebou pro takovou osobu nést právní důsledky či na ni mohou mít značný negativní vliv, nesmí být založena pouze na automatizovaném zpracování. Subjekt údajů má právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká. To se týká zejména rozhodnutí, pro něž jsou důležité údaje o odborné způsobilosti či zdravotním stavu subjektu údajů. Tento odstavec se nepoužije, pokud je rozhodnutí:
 - a) nezbytné k uzavření nebo plnění smlouvy mezi subjektem údajů a správcem údajů;
 - b) povoleno právem Evropské unie nebo právem České republiky, které se na správce vztahuje a které rovněž stanoví vhodná opatření zajišťující ochranu práv a svobod a oprávněných zájmů subjektu údajů; nebo
 - c) založeno na výslovném souhlasu subjektu údajů.
2. Pokud bude v individuálních případech automatizované rozhodnutí objektivně nutné, bude subjekt údajů o jeho výsledku bezodkladně informován a bude mu poskytnuta příležitost se k němu v přiměřené časové lhůtě vyjádřit. Vyjádření subjektu údajů bude před přijetím finálního rozhodnutí vzato adekvátním způsobem v úvahu.

Proces ukládání údajů ve společnosti

1. Osobní údaje jsou ve společnosti zanášeny pověřenými zaměstnanci a externími spolupracovníky strukturovaně do IT systému. Automatizovaně jsou zachycovány na záznamech z kamerového systému, v souboru životopisů uchazečů o zaměstnání, v docházkovém systému apod. Postup pro zpracování údajů z kamerového systému je popsán v samostatné směrnici.
2. Přístup k bázím s osobními údaji je ošetřen přístupovými právy, která spravuje oddělení/dodavatel IT ve spolupráci se správcem údajů a tento postup je upraven v samostatné směrnici LPT-IP-5. Všichni zaměstnanci, kteří mají přístup k těmto databázím s údaji jsou poučeni o zachování mlčenlivosti a o správném nakládání s údaji.
3. Zpracování údajů v IT systému probíhá na serveru, který je umístěn v LPT-IP-5. Přenos údajů je realizován v součinnosti se zástupcem zpracovatele po datových sítích.

Zvláštní kategorie osobních údajů

1. Pro nakládání s osobními údaji zvláštní kategorie je nutné výslovné oprávnění na právním základě či předchozí souhlas subjektu údajů. Nakládání s osobními údaji zvláštní kategorie je rovněž dovoleno, je-li nutné pro zpracování údajů za účelem naplnění práv a splnění povinností příslušného subjektu v oblasti pracovního práva, dovoluje-li to právo daného státu poskytující příslušné záruky.
2. Před zahájením shromažďování, zpracovávání či využívání takovýchto údajů je ve všech potřebných případech nutná řádná písemná konzultace s místem společnosti odpovědným za ochranu údajů. Měla by být řádně zohledněna povaha, rozsah, účel, nutnost a právní podklad použití údajů.

6 Práva subjektů údajů

i. Právo na dotazy a stížnosti

1. Každý subjekt údajů je oprávněn kdykoli kontaktovat příslušné místo společnosti odpovědné za ochranu údajů s dotazy a stížnostmi v souvislosti se zákonem a aplikací tohoto Kodexu. Není-li následně uvedeno jinak, je pro účely těchto ustanovení odpovědnou společností jakákoli společnost, která je ve smluvním vztahu se subjektem údajů či která zpracovává osobní údaje subjektu údajů.

ii. Právo na přístup a informace

1. Každý subjekt údajů je oprávněn si kdykoli vyžádat informace týkající se:
 - a) uložených osobních údajů, včetně jejich původu a příjemce (příjemců);
 - b) účelu jejich zpracování či použití;
 - c) příjemců a kategorií příjemců, kterým jsou osobní údaje subjektu údajů předávány, zejména v případě jejich předávání do zahraničí;
 - d) plánované doby, po kterou budou osobní údaje uloženy;
 - e) existence práva požadovat od správce opravu nebo výmaz osobních údajů, právo vznést námitku;
 - f) právo podat stížnost u dozorového úřadu;
 - g) veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů;
 - h) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování;
 - ch) ustanovení tohoto Kodexu.
2. Tyto informace by měly být příslušnému subjektu údajů, který o ně projeví zájem, sděleny ve srozumitelné podobě, v přiměřené časové lhůtě, nejdéle do 1 měsíce a v odůvodněných případech do 3 měsíců a měly by mu být poskytnuty v písemné či elektronické podobě.
3. V případech, kdy je žádost o poskytnutí informací zjevně nedůvodná nebo nepřiměřená, zejména protože se opakuje, tak si může společnost za poskytnutí příslušné informace účtovat poplatek.

iii. Právo na vznesení námitky/výmaz údajů/blokování údajů

1. Pokud je k tomu oprávněn, může příslušný subjekt údajů vznést vůči odpovědné společnosti námitku proti použití jeho údajů, a to v případech kdy:
 - a) zpracování je nezbytné pro plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen,
 - b) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany.
2. Toto právo na vznesení námitky se vztahuje i na případy, kdy subjekt údajů s použitím svých údajů dříve souhlasil.
3. Oprávněné žádosti o výmaz či blokování údajů budou bez zbytečného odkladu, za splnění zákonných podmínek, kladně vyřízeny. Takovéto žádosti jsou oprávněné zejména tehdy, pomínou-li právní důvody pro použití údajů. Má-li subjekt údajů na výmaz údajů právo, ale není-li výmaz možný nebo není možný při vynaložení přiměřeného úsilí, budou údaje chráněny proti nepovolenému užití blokováním. Zákonné lhůty pro uchování údajů budou dodržovány.

iv. Právo na opravu

1. Subjekt údajů může kdykoli požádat, aby společnost opravila jeho osobní údaje zaznamenané společností v případě, že tyto údaje jsou neúplné a/nebo nesprávné.

v. Právo na vysvětlení a komentář

1. V případě tvrzení subjektu údajů, že byla porušena jeho práva v důsledku nezákonného zpracování údajů, zejména pak v případě porušení tohoto Kodexu, objasní společnosti bez zbytečného odkladu okolnosti případu. V takovémto případě spolu budou úzce spolupracovat a umožní jeden druhému přístup ke všem informacím, jež jsou nezbytné za účelem zjištění okolností případu.
2. Oddělení společnosti odpovědné za ochranu údajů, kterého se záležitost nejbližší týká, musí koordinovat veškerou příslušnou korespondenci se subjektem údajů.

vi. Právo na přenositelnost osobních údajů

1. Přenositelností osobních údajů je právo subjektu údajů, jehož podstatou je možnost za určitých podmínek získat osobní údaje, které se ho týkají a jež společnosti poskytl, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jiné společnosti - správci, aniž by tomu původní společnost bránila. Zároveň má subjekt údajů, pokud požádá, i právo na to, aby společnost předala jeho osobní údaje ve strukturovaném, běžně používaném a strojově čitelném formátu jiné společnosti, je-li to technicky proveditelné.
2. Právo přenositelnosti osobních údajů může být aplikováno pokud:
 - a) jde o zpracování osobních údajů založené na právním důvodu, souhlasu či smlouvě,
 - b) zpracování se provádí automatizovaně.

Výkon práv subjektů údajů

1. Subjekty údajů nebudou z důvodu využití těchto práv znevýhodněny. Způsob komunikace se subjektem údajů – např. telefonický, elektronický či písemný kontakt – by měl v příslušných případech brát ohled na požadavek subjektu údajů.

7 Proces řízení správy, zpracování a ochrany údajů/Odpovědnost za ochranu údajů

Ve společnosti shromažďují a zpracovávají údaje na jedné straně zaměstnanci společnosti a dále také dochází ke shromažďování a zpracování osobních údajů skrze externí osoby.

i. Odpovědnost za správu a zpracování údajů

1. Společnost má ve své funkci vedoucího zaměstnance/správce údajů, který má povinnost zajišťovat dodržování požadavků na ochranu údajů a ustanovení tohoto Kodexu, a to zejména ve vztahu k subjektům údajů a zákonným povinnostem. Správce údajů dále zajišťuje a rozhoduje o správě a zpracování údajů určených zákony (např. zákoníkem práce, zákonem o účetnictví, zákonem o daních z příjmů, zákonem o zdravotním pojištění, zákonem o organizaci a provádění sociálního zabezpečení, zákonem o důchodovém pojištění, zákonem o archivnictví atd.)
2. Osoba společnost odpovědná za ochranu údajů bude bezodkladně informována o jakémkoli porušení (včetně podezření) předpisů o ochraně údajů a ustanovení tohoto Kodexu.
3. Oddělení/osoba odpovědné/á za ochranu údajů společnosti bude koordinovat aktivity v rámci strategie ochrany údajů společnosti.
4. Administrativní pracovník, který shromažďuje a zpracovává údaje ostatních zaměstnanců, je oprávněn vést pouze ty údaje, které jsou blíže specifikované v příloze č. 1 tohoto kodexu.

Administrativní pracovník rovněž zajišťuje shromažďování a správu smluvních dokumentů s obchodními partnery od jejich uložení až po skartační řízení, jehož proces je popsán v samostatné směrnici.

5. Údaje o poskytování pracovně lékařských služeb subjektu údajů a o všech úkonech s touto péčí souvisejících vede v souladu s právními předpisy poskytovatel pracovně lékařských služeb. Spravovat údaje / zpracovávat údaje o zdravotní způsobilosti subjektu údajů je oprávněn pouze poskytovatel pracovně lékařských služeb. Předat, šířit či zveřejňovat může poskytovatel pracovně lékařských služeb pouze údaje odpovídající stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu.

ii. Proces řízení správy, zpracování a ochrany údajů

1. V případě potřeby jiného zaměstnance/ oddělení / organizační jednotky nakládat s údaji je takový zaměstnanec / oddělení / org. jednotka oprávněn / -á pouze se souhlasem správce údajů a pouze s údaji, které jsou nezbytně nutné. Správce údajů (vedoucí, pověřený zaměstnanec) musí vždy zvážit důvodnost vzneseného požadavku a případně ho i odmítnout. O předání údajů se sepisuje záznam.
2. Shledá-li správce údajů údaje nezbytnými, informuje vedoucího společnosti, který zabezpečí případnou oznamovací povinnost Úřadu na ochranu osobních údajů dle zákona o ochraně osobních údajů. Po registraci Úřadem na ochranu osobních údajů postupuje správce údajů stejně jako u vynucených údajů, tj. definuje jejich účel a promítne je do přílohy č. 1 tohoto kodexu. Oprávněnému zaměstnanci nechá podepsat prohlášení o mlčenlivosti, proškolí ho a v případě automatizovaného zpracování údajů zajistí příslušná přístupová práva do systému.

Povinnost dozoru a konzultací

1. Osoba společnosti odpovědná za ochranu údajů / správce údajů je povinna sledovat, zda jsou dodržovány národní a mezinárodní předpisy upravující ochranu údajů a tento Kodex. V tomto ohledu budou veškerá oddělení společnosti povinna informovat příslušnou osobu odpovědnou za ochranu údajů o příslušném vývoji a plánech do budoucna.
2. Nebudou-li tomu bránit právní překážky, je příslušná osoba odpovědná za ochranu údajů oprávněna přímo na místě přezkoumat veškeré techniky pro zpracování dat, při nichž jsou využívány osobní údaje.

Vedoucí zaměstnanci společnosti

Vedoucí zaměstnanci společnosti shromažďují a zpracovávají údaje svých podřízených zaměstnanců při plnění pracovních činností, a to v souladu se zákonem. O veškerých skutečnostech, o kterých se při zpracování údajů dozví, jsou povinni zachovat mlčenlivost dle podepsané dohody o mlčenlivosti.

Proškolení zaměstnanců

1. Zaměstnanci společnosti jsou dostatečně proškoleni ve znalosti předpisů na ochranu údajů a aplikaci tohoto Kodexu.
2. Ve spolupráci s příslušnými odděleními/osobami odpovědnými za ochranu údajů vypracovává společnost pro takovéto školení vhodné materiály.

Spolupráce s příslušnými orgány veřejné správy

1. Společnost se zavazuje, že v přiměřené časové lhůtě a přiměřeném rozsahu zodpoví dotazy příslušnému orgánu veřejné správy, který je za ně odpovědný či který je případně odpovědný za společnost předávající údaje, a že se budou řídit doporučeními tohoto orgánu.

iii. Postup v případě úniku či zcizení osobních údajů

1. Jakékoli narušení bezpečnosti osobních údajů společnost bez zbytečného odkladu ohlašuje dozorovému úřadu (ÚOOÚ), a to nejdéle do 72 hodin. V odůvodněných případech společnost může činit i déle.
2. Společnost má pro řešení narušení bezpečnosti osobních údajů nastaveny procesy řešení těchto incidentů. Společnost zajišťuje procesy a technologie, které umožňují odhalit případy porušení zabezpečení osobních údajů, umožňují zareagovat na ně a zajistit nápravu.
3. Ohlašování narušení bezpečnosti osobních údajů obsahuje:
 - a) popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů.
 - b) Jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace,
 - c) Popis pravděpodobných důsledků porušení zabezpečení osobních údajů,
 - d) Popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.
4. Společnost nemusí hlásit narušení bezpečnosti osobních údajů v případě, že by narušení bezpečnosti osobních údajů nemělo za následek riziko pro práva a svobody fyzických osob.

iv. Posouzení vlivu na ochranu osobních údajů (PIA)

1. PIA je nástroj určený pro identifikaci a vyhodnocení rizik o ochraně osobních údajů.
2. Tam, kde je riziko narušení soukromí vysoké a je tedy potřeba rizika pro subjekty údajů minimalizovat společnost identifikuje a vyhodnocuje rizika o ochraně osobních údajů.

8 Kamerový systém společnosti

Společnost neprovozuje kamerový systém.

9 Odpovědnost za porušení povinností stanovených tímto Kodexem

Porušení povinností uvedených v tomto Kodexu a povinnosti mlčenlivosti zaměstnanci společnosti bude kvalifikováno jako porušení pracovní kázně podle § 301 a § 302 ZPr s možností postihu podle zákona a zejména dle § 52, příp. § 55 ZPr.

Jakékoli správně právní a soukromoprávní postihy společnosti v důsledku nedodržení povinností zaměstnanců a jiných odpovědných osob podle tohoto Kodexu budou v plném rozsahu uplatňovány vůči těmto osobám.

Tím není dotčeno právo zaměstnavatele na náhradu škody vůči zaměstnanci ani právo poškozeného subjektu údajů domáhat se práva na ochranu osobnosti podle § 81 a násl. a § 2894 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

10 Změny kodexu

Za změny tohoto kodexu zodpovídá Ing. Lucie Petráková.